Title/Subject: **HIPAA: PROTECTING ELECTRONIC PROTECTED HEALTH INFORMATION POLICY**

Title/Subject: HIPAA: **PROTECTING ELECTRONIC PROTECTED HEALTH INFORMATION POLICY**

Applies to: ☒ faculty ☒ staff ☒ students ☒ student employees ☐ visitors ☒ contractors

Effective Date of This Revision: November 21, 2019

Contact for More Information: **Office of HIPAA Compliance**
989-774-2829
hipaa@cmich.edu

☐ Board Policy ☒ Administrative Policy ☐ Procedure ☐ Guideline

BACKGROUND:

Central Michigan University (CMU) is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) law and regulations. CMU's business activities include both covered and non-covered functions. CMU has decided to designate itself as a Hybrid Entity.

According to the law, all CMU officers, employees and agents of units within the Hybrid Entity must preserve the integrity and confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client. This IIHI is considered protected health information (PHI) and shall be safeguarded in compliance with the requirements of the Security and Privacy rules and standards established under HIPAA.

For additional information on the measures Central Michigan University is implementing in order to comply with this legislation, visit CMU's official HIPAA web site at HIPAA.cmich.edu.

PURPOSE:

This policy establishes how CMU has and will comply with the HIPAA Security regulations and includes what measures have been or will be implemented to remain compliant. Compliance by all units within CMU's Hybrid Entity is required. For CMU, this policy applies if IIHI is obtained by a unit within CMU's Hybrid Entity. In addition, some units may elect to protect PHI within the secured network, even if they are not a part of the Hybrid Entity. In those cases, these policies will also apply.

DEFINITIONS:

Hybrid Entity. A department or unit designated within the Hybrid Definition (See Policy 12-2: HIPAA Hybrid Entity Defined at HIPAA.cmich.edu).

Protected Health Information Network (PHIN). The secured network established by CMU for HIPAA protected health information. This network consists of appropriately protected segments of the broader CMU network and appropriately protected extensions established as a result of contractual relationships with third-party providers. Access to this network is only available from HIPAA workstations by authorized personnel who have been properly trained and granted the access appropriate to their job.

Authority: Robert O. Davies, President
History: 2005-03-30; 2018-11-16
Indexed as: HIPAA Workstation; HIPAA Personal Security Policy; HIPAA Security Policy

Individually Identifiable Health Information (IIHI). A subset of health information, including demographic information collected from a patient/client/employee, that is created or received by a health care provider, health plan or employer and relates to the past, present, or future physical or mental health or condition of a patient/client/employee, the provision of health care to a patient/client/employee, or the past, present or future payment for the provision of health care to a patient/client/employee, and which identifies the patient/client/employee, or with respect to which there is a reasonable basis to believe that the information can be used to identify the patient/client/employee.

Electronic Protected Health Information (ePHI). Individually identifiable health information (IIHI) that is transmitted by electronic media; maintained in electronic media, such as magnetic tape, disc, optical file; or transmitted or maintained in any other form or medium, except that it does not include IIHI in education records covered by the Family Educational Rights and Privacy Act, certain treatment records of CMU students as described at 20 USC 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer.

Workforce Member. A "Workforce Member" includes employees (and student employees), volunteers, trainees, and other persons whose conduct, in the performance of work for a unit in the CMU Hybrid entity is under the direct control of such entity, whether or not they are paid by the entity. This includes students who have access to PHI in order to satisfy a clinical experience requirement for a program of study.

All other terms used in this policy have the same meaning as those terms in the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 and the regulations at 45 CFR Parts 160, 162, and 164.

POLICY:

1.0 All Workforce Members within CMU's HIPAA Hybrid Entity are responsible for maintaining the privacy and security of all Electronic Protected Health Information (ePHI) at all times and in all locations. To help maintain a high level of security for protecting ePHI, HIPAA Workforce Members shall adhere to the strategy the Office of Information Technology (OIT) has identified below. In addition, also see Safeguards policy #12-13 for protecting IIHI in other media (oral, paper).

2.0 CMU has adopted the following general strategy as a mechanism for protecting ePHI:

a. OIT maintains a Protected Health Information Network (PHIN) as an added layer of defense to protect CMU's ePHI.
b. ePHI should only be stored on systems hosted on the PHIN or covered by a Business Associate Agreement.
c. Whenever possible, ePHI shall remain in its primary host system. (Refer to the HIPAA unit's training protocol and procedures for maintaining communication within the Electronic Medical Record (EMR) systems).
d. ePHI removed from its host system, for any reason, must be encrypted both at rest and in transit.
e. ePHI should only be accessed from approved devices/systems that have appropriate security controls in place.
f. The HIPAA Privacy Officer and the HIPAA Security Officer will jointly maintain procedures and guidelines for the protection of ePHI.
    i. The procedures and guidelines noted below will inherit or strengthen the requirements found in CMU's Secure Configurations – Workstations Policy #3-49, including, but not limited to those for malware defense and encryption. https://www.cmich.edu/office_president/general_counsel/Documents/p03049.pdf
    ii. The procedures and guidelines noted below will inherit password controls from CMU's Password Policy #3-48. https://www.cmich.edu/office_president/general_counsel/Documents/p03048.pdf
    iii. Also see Safeguards Policy #12-13 at HIPAA.cmich.edu